

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-296394
(43)Date of publication of application : 29.10.1999

(51)Int.Cl. G06F 11/18

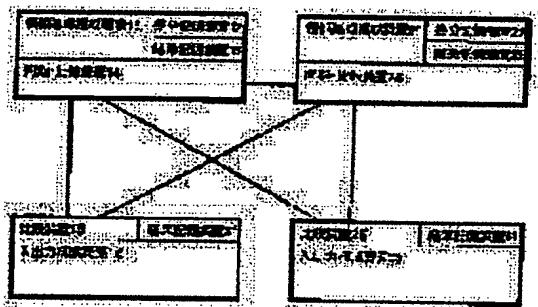
(21)Application number : 10-104746 (71)Applicant : NEC CORP
(22)Date of filing : 15.04.1998 (72)Inventor : KOGURE AKIRA

(54) DUPLEX INFORMATION PROCESSOR

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a countermeasure to a transition fault or an intermittent fault due to a disturbing factor incurring the minimum cost in a normal redundant computer system in which hardware is duplexed.

SOLUTION: In this duplex information processor, when the operations or outputs of first and second information processing constituting elements 11 and 21 are not made coincident, and generation of a fault is not detected in any information processing constituting element, re-execution is operated. Afterwards, when the operations or outputs of the information constituting elements are not made coincident, and generation of a fault is not detected in any information processing constituting element, the output result is compared with the result of incoincidence stored in result storing means 13 and 23 for each information processing constituting element. Thus, the operational constitution of the system can be decided according to the compared result.



(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平11-296394

(43)公開日 平成11年(1999)10月29日

(51)Int.Cl.⁸
G 0 6 F 11/18

識別記号
3 1 0

F I
G 0 6 F 11/18

3 1 0 C
3 1 0 G

審査請求 有 請求項の数8 OL (全12頁)

(21)出願番号 特願平10-104746

(22)出願日 平成10年(1998)4月15日

(71)出願人 000004237
日本電気株式会社
東京都港区芝五丁目7番1号

(72)発明者 小暮 晃
東京都港区芝五丁目7番1号 日本電気株式会社内

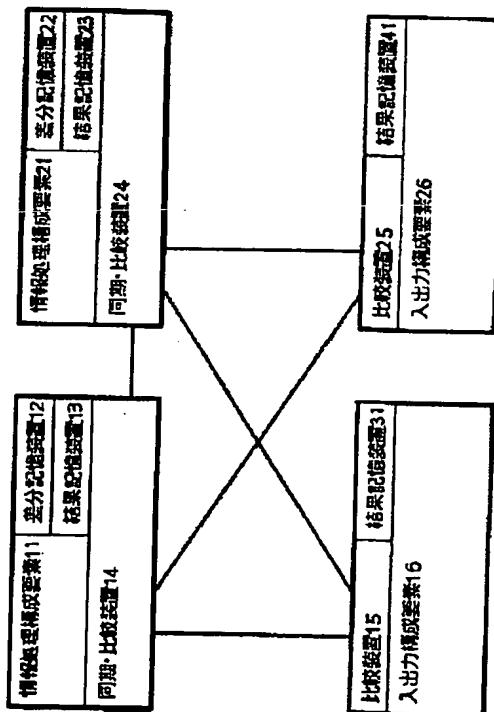
(74)代理人 弁理士 山下 積平

(54)【発明の名称】二重化情報処理装置

(57)【要約】

【課題】 ハードウェアを二重化した常用冗長コンピュータシステムにおいて、最小限のコスト追加により外乱要因による過渡フォールトや間欠フォールトへの対策を提供する。

【解決手段】 第1及び第2の情報処理構成要素11, 21の動作又は出力に不一致があり、いずれの情報処理構成要素にもフォールトの発生が検出されない場合に、再実行の後、なお、情報処理構成要素どうしの動作又は出力に不一致があり、いずれの情報処理構成要素にも、フォールトの発生が検出されないときに、各情報処理構成要素毎に、出力結果と上記結果記憶手段13, 23に記憶された不一致結果とを、それぞれ比較することにより、該比較結果に応じてシステムの運用構成を決定する手段と、を有することを特徴とする二重化情報処理装置。



【特許請求の範囲】

【請求項1】 ハードウェアを二重化した常用冗長コンピュータシステムにおいて、

第1及び第2の情報処理構成要素の動作又は出力に不一致があり、いずれの情報処理構成要素にもフォールトの発生が検出されない場合に、

上記不一致が発生した結果を、それぞれ、対応する情報処理構成要素において記憶しておくための結果記憶手段と、

再実行の後、なお、第1及び第2の情報処理構成要素の動作又は出力に不一致があり、いずれの情報処理構成要素にも、フォールトの発生が検出されないときに、各情報処理構成要素毎に、出力結果と上記結果記憶手段に記憶された不一致結果とを、それぞれ比較する手段と、該比較結果に応じてシステムの運用構成を決定する手段と、を有することを特徴とする二重化情報処理装置。

【請求項2】 ハードウェアを二重化した常用冗長コンピュータシステムにおいて、

第1及び第2の入出力構成要素の動作又は出力に不一致があり、いずれの入出力構成要素にもフォールトの発生が検出されない場合に、

上記不一致が発生した結果を、それぞれ、対応する入出力構成要素において記憶しておくための結果記憶手段と、

再実行の後、なお、第1及び第2の入出力構成要素の動作又は出力に不一致があり、いずれの入出力構成要素にも、フォールトの発生が検出されないときに、各入出力構成要素毎に、出力結果と上記結果記憶手段に記憶された不一致結果とを、それぞれ比較する手段と、

該比較結果に応じてシステムの運用構成を決定する手段と、を有することを特徴とする二重化情報処理装置。

【請求項3】 請求項2記載の入出力構成要素を有することを特徴とする請求項1記載の二重化情報処理装置。

【請求項4】 ハードウェアを二重化した常用冗長コンピュータシステムにおいて、

二重化された情報処理構成要素(11, 21)を有し、前記情報処理構成要素(11, 21)は、それぞれ、該情報処理構成要素(11, 21)どうしの動作の一一致、または出力の一一致を比較する手段(14, 24)と、該情報処理構成要素どうし(11, 21)の動作の一一致、または出力の一一致が確認された状態と、確認される前の状態との差分情報を記憶しておく差分記憶装置(12, 22)と、

該情報処理構成要素(11, 21)の動作結果、又は出力結果を記憶しておくための結果記憶装置(13, 23)と、

該情報処理構成要素(11, 21)どうしの動作の不一致、または出力の不一致を検出した場合に、

前記差分記憶装置(12, 22)の情報を元に、それぞれの前記情報処理構成要素(11, 21)を、前記不一致が検出される前の状態に戻し、複数回の再実行を行なう手段と、

それぞれの前記情報処理構成要素(11, 21)内において、前記再実行後の結果と再実行前の結果とを比較する手段と、

該比較結果に応じてシステムの運用構成を決定する手段と、を有することを特徴とする請求項1記載の二重化情報処理装置。

【請求項5】 前記比較結果に応じてシステムの運用構成を決定する手段は、

前記比較の結果、前記情報処理構成要素(11, 21)どうしの動作の不一致、または出力の不一致を検出した場合に、

それぞれの該情報処理構成要素(11, 21)のどちらか一方でフォールトの発生が検出されていれば、フォールトの発生した情報処理要素を切り離して縮退運用を行ない、

フォールトの発生が検出されていなければ、それぞれの前記結果記憶装置(13, 23)に、それぞれの情報処理構成要素(11, 21)の状態を記憶した後、それぞれの差分記憶装置(12, 22)の情報を元に、前記不一致が検出される前の状態に戻し、複数回の再実行を行なう手段と、

最初の再実行で、前記情報処理構成要素(11, 21)どうしの動作の一一致、または出力の一一致が確認されれば、フォールトは、外乱要因による過渡的なものと判断し、そのまま処理を継続し、

最初の再実行で、再度、不一致が検出された場合には、それぞれの情報処理構成要素(11, 21)の出力結果と、それぞれの結果記憶装置(13, 23)に記憶されていた出力結果との比較を行なう手段と、

該比較の結果、それぞれの前記情報処理構成要素(11, 21)の一方が一致して、他方が一致していないければ、一致していない方の情報処理構成要素を切り離して縮退運用を行ない、

両方とも不一致であれば、二重の固定的または間欠的なフォールトが発生したと判断し、その時点で運用を停止し、

両方とも一致していれば、指定された回数だけ再実行を繰り返し、全ての再実行において、該情報処理構成要素(11, 21)どうしの出力結果に不一致があり、かつ、該出力結果が、それぞれの結果記憶装置(13, 23)に記憶された結果と一致していれば、フォールトの発生箇所が特定できない致命的な固定フォールトが発生したと判断し、その時点で運用を停止する手段と、を有することを特徴とする請求項4記載の二重化情報処理装置。

【請求項6】 ハードウェアを二重化した常用冗長コンピュータシステムにおいて、

二重化された入出力構成要素(16, 26)を有し、

それぞれの前記入出力構成要素(16, 26)どうしの出力の一致を比較する手段(15, 25)と、該入出力構成要素(16, 26)の出力結果を記憶しておくための結果記憶装置(31, 41)と、前記比較結果に応じてシステムの運用構成を決定する手段と、を有することを特徴とする請求項2記載の二重化情報処理装置。

【請求項7】 前記比較結果に応じてシステムの運用構成を決定する手段は、

前記比較の結果、入出力構成要素(16, 26)の出力の不一致が検出された場合、入出力構成要素(16, 26)のどちらか一方でフォールトの発生が検出されれば、フォールトの発生した入出力構成要素を切り離して縮退運用を行ない、

フォールトの発生が検出されていなければ、それぞれの前記結果記憶装置(31, 41)に、入出力構成要素(16, 26)の出力を記憶した後、入出力処理の複数回の再実行を行ない、

最初の再実行で、入出力構成要素(16, 26)の出力の一致が確認されれば、フォールトは、過渡的なものと判断し、そのまま処理を継続し、

再度、不一致が検出された場合には、それぞれの入出力構成要素(16)の出力結果と結果記憶装置(31)に記憶しておいた結果とで、比較を行ない、入出力構成要素(16, 26)の一方が一致して、他方が一致していなければ、一致していない方の入出力構成要素を切り離して縮退運用を行ない、

両方とも不一致であれば、原理的に二重化常用冗長コンピュータシステムでは対処できない二重の固定的または間欠的なフォールトが発生したと判断し、その時点で運用を停止し、

両方とも一致していれば、指定された回数だけ再実行を繰り返し、全ての再実行において、入出力構成要素どうしに不一致があり、かつ結果記憶装置とも一致していれば、フォールトの発生箇所が特定できない致命的な固定フォールトが発生したと判断し、その時点で運用を停止する手段と、を有することを特徴とする請求項6記載の二重化情報処理装置。

【請求項8】 前記フォールトの発生箇所が特定できない場合に限り、前記再実行を行なう、ことを特徴とした請求項1～7のいずれかに記載の二重化情報処理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ハードウェアを二重化した常用冗長コンピュータシステムに関する。

【0002】

【従来の技術】従来の、ハードウェアを二重化した常用冗長コンピュータシステムについて、図2を参照して説明する。

【0003】図2において、同期・比較装置102と同

期・比較装置202は、互いに協調し合い、情報処理構成要素101と情報処理構成要素201の動作を同期させると共に、情報処理構成要素101と情報処理構成要素201の動作が一致しているかの比較を行なう。

【0004】また、入出力構成要素104と入出力構成要素204の出力を、同期・比較装置102と同期・比較装置202を経由して受け取り、比較の結果が一致していれば、情報処理構成要素101と情報処理構成要素201に入力する。

10 【0005】さらに、情報処理構成要素101と情報処理構成要素201の出力は、比較装置103と比較装置203を経由して、比較の結果が一致していれば、入出力構成要素104と入出力構成要素204に入力する。

【0006】もし、情報処理構成要素101と情報処理構成要素201の動作の一一致、または出力の一一致を確認した際に不一致が検出された場合、情報処理構成要素101と情報処理構成要素201のどちらか一方でフォールトの発生が検出されれば、フォールトの発生した情報処理構成要素を切り離して、縮退運用を行なう。

20 【0007】フォールトの発生が検出されていなければ、フォールトの発生箇所が特定できない致命的な固定フォールトが発生したと判断して、その時点で運用を停止するか、情報処理構成要素101か情報処理構成要素201のどちらかが正しいと想定し、他方を切り離して縮退運用を行なう。

【0008】また、もし入出力構成要素104と入出力構成要素204の出力の一一致を確認した際に、不一致が検出された場合、入出力構成要素104と入出力構成要素204のどちらか一方でフォールトの発生が検出されれば、フォールトの発生した入出力構成要素を切り離して縮退運用を行なう。フォールトの発生が検出されていなければ、入出力処理の再実行を行なう。

【0009】最初の再実行で、入出力構成要素104と入出力構成要素204の出力の一一致が確認されれば、フォールトは外乱要因による過渡的なものと判断し、そのまま処理を継続する。

【0010】しかし、再度、不一致が検出された場合には、フォールトの発生箇所が特定できない致命的な固定フォールトが発生したと判断して、その時点で運用を停止するか、入出力構成要素104か入出力構成要素204のどちらかが正しいと想定し、他方を切り離して縮退運用を行なう。

【0011】また、特開平4-71037号公報、及び特開平4-71038号公報には、2つのCPUの出力データの各々に不一致があった場合に、リトライ処理を所定回行なうようにした電子計算機の二重化方式が開示されている。具体的には、データ再送のリトライ、タスクレベルでのリトライ、及びOSによるテストプログラム実行を逐次行なわせている。

【0012】また、特開平9-55797号公報には、

障害解析自動診断処理方法として、運用系と待機系とかなる二重化装置に関するものが開示され、障害が発生した1つの装置内において、障害箇所の特定を行なっている。

【0013】

【発明が解決しようとする課題】しかしながら、従来のハードウェアを二重化した常用冗長コンピュータシステムにおいては、次のような課題がある。

【0014】第1の課題は、ハードウェアの二重化以外の冗長手段を持たない為、フォールトの発生個所が特定できなければ、外乱要因による過渡フォールトや、ハードウェア故障と外乱要因の複合条件により発生する間欠フォールトを、無条件に致命的なフォールトとして扱わざるを得ないことである。

【0015】近年は、半導体の集積度向上、動作電圧の低下、動作周波数の向上、携帯電話やモバイル機器の普及など、外乱要因による過渡フォールトや間欠フォールトの発生する確率が増加してきており、何らかの対策を講じる必要があった。第2の課題は、三重化以上のハードウェアで、常用冗長コンピュータシステムを構成すれば、第1の課題は解決できるものの、どうしても大幅なコストの上昇が避けられないということである。

【0016】フォールトの発生個所を特定する技術は、年々進歩してきており、フォールトの発生個所を特定する為だけに高価な三重化以上のハードウェアを装備することは、価格を度外視して信頼性を重視するニッチな用途向けとなりつつある。

【0017】また、特開平4-71037号公報、及び特開平4-71038号公報には、2つのCPUの出力データの各々に不一致があった場合に、リトライ処理を所定回行なうようにした電子計算機の二重化方式が開示されているに過ぎない。

【0018】また、特開平9-55797号公報には、障害解析自動診断処理方法として、運用系と待機系とかなる二重化装置に関するものが開示され、障害が発生した1つの装置内において、障害箇所の特定を行なっているに過ぎない。

【0019】【発明の目的】本発明の目的は、ハードウェアを二重化した常用冗長コンピュータシステムにおいて、最小限のコスト追加により外乱要因による過渡フォールトや間欠フォールトへの対策を提供することにある。

【0020】

【課題を解決するための手段】本発明は、上記課題を解決するための手段として、ハードウェアを二重化した常用冗長コンピュータシステムにおいて、第1及び第2の情報処理構成要素の動作又は出力に不一致があり、いずれの情報処理構成要素にもフォールトの発生が検出されない場合に、上記不一致が発生した結果を、それぞれ、対応する情報処理構成要素において記憶しておくための

結果記憶手段と、再実行の後、なお、第1及び第2の情報処理構成要素の動作又は出力に不一致があり、いずれの情報処理構成要素にも、フォールトの発生が検出されないときに、各情報処理構成要素毎に、出力結果と上記結果記憶手段に記憶された不一致結果とを、それぞれ比較する手段と、該比較結果に応じてシステムの運用構成を決定する手段と、を有することを特徴とする二重化情報処理装置を提供するものである。

【0021】また、ハードウェアを二重化した常用冗長コンピュータシステムにおいて、第1及び第2の入出力構成要素の動作又は出力に不一致があり、いずれの入出力構成要素にもフォールトの発生が検出されない場合に、上記不一致が発生した結果を、それぞれ、対応する入出力構成要素において記憶しておくための結果記憶手段と、再実行の後、なお、第1及び第2の入出力構成要素の動作又は出力に不一致があり、いずれの入出力構成要素にも、フォールトの発生が検出されないときに、各入出力構成要素毎に、出力結果と上記結果記憶手段に記憶された不一致結果とを、それぞれ比較する手段と、該比較結果に応じてシステムの運用構成を決定する手段と、を有することを特徴とする二重化情報処理装置もある。

【0022】また、上記情報処理構成要素と上記入出力構成要素との両方を有することを特徴とする二重化情報処理装置もある。

【0023】また、ハードウェアを二重化した常用冗長コンピュータシステムにおいて、二重化された情報処理構成要素(11, 21)を有し、前記情報処理構成要素(11, 21)は、それぞれ、該情報処理構成要素(11, 21)どうしの動作の一一致、または出力の一一致を比較する手段(14, 24)と、該情報処理構成要素どうし(11, 21)の動作の一一致、または出力の一一致が確認された状態と、確認される前の状態との差分情報を記憶しておく差分記憶装置(12, 22)と、該情報処理構成要素(11, 21)の動作結果、又は出力結果を記憶しておくための結果記憶装置(13, 23)と、該情報処理構成要素(11, 21)どうしの動作の不一致、または出力の不一致を検出した場合に、前記差分記憶装置(12, 22)の情報を元に、それぞれの前記情報処理構成要素(11, 21)を、前記不一致が検出される前の状態に戻し、複数回の再実行を行なう手段と、それぞれの前記情報処理構成要素(11, 21)内において、前記再実行後の結果と再実行前の結果とを比較する手段と、該比較結果に応じてシステムの運用構成を決定する手段と、を有することを特徴とする二重化情報処理装置もある。

【0024】また、前記比較結果に応じてシステムの運用構成を決定する手段は、前記比較の結果、前記情報処理構成要素(11, 21)どうしの動作の不一致、または出力の不一致を検出した場合に、それぞれの該情報処理構成要素(11, 21)を、前記不一致が検出される前の状態に戻し、複数回の再実行を行なう手段と、それぞれの前記情報処理構成要素(11, 21)内において、前記再実行後の結果と再実行前の結果とを比較する手段と、該比較結果に応じてシステムの運用構成を決定する手段と、を有することを特徴とする二重化情報処理装置もある。

【0025】また、前記比較結果に応じてシステムの運用構成を決定する手段は、前記比較の結果、前記情報処理構成要素(11, 21)どうしの動作の不一致、または出力の不一致を検出した場合に、それぞれの該情報処理構成要素(11, 21)を、前記不一致が検出される前の状態に戻し、複数回の再実行を行なう手段と、それぞれの前記情報処理構成要素(11, 21)内において、前記再実行後の結果と再実行前の結果とを比較する手段と、該比較結果に応じてシステムの運用構成を決定する手段と、を有することを特徴とする二重化情報処理装置もある。

理構成要素(11, 21)のどちらか一方でフォールトの発生が検出されていれば、フォールトの発生した情報処理要素を切り離して縮退運用を行ない、フォールトの発生が検出されていなければ、それぞれの前記結果記憶装置(13, 23)に、それぞれの情報処理構成要素(11, 21)の状態を記憶した後、それぞれの差分記憶装置(12, 22)の情報を元に、前記不一致が検出される前の状態に戻し、複数回の再実行を行なう手段と、最初の再実行で、前記情報処理構成要素(11, 21)どうしの動作の一一致、または出力の一一致が確認されれば、フォールトは、外乱要因による過渡的なものと判断し、そのまま処理を継続し、最初の再実行で、再度、不一致が検出された場合には、それぞれの情報処理構成要素(11, 21)の出力結果と、それぞれの結果記憶装置(13, 23)に記憶されていた出力結果との比較を行なう手段と、該比較の結果、それぞれの前記情報処理構成要素(11, 21)の一方が一致して、他方が一致していなければ、一致していない方の情報処理構成要素を切り離して縮退運用を行ない、両方とも不一致であれば、二重の固定的または間欠的なフォールトが発生したと判断し、その時点で運用を停止し、両方とも一致していれば、指定された回数だけ再実行を繰り返し、全ての再実行において、該情報処理構成要素(11, 21)どうしの出力結果に不一致があり、かつ、該出力結果が、それぞれの結果記憶装置(13, 23)に記憶された結果と一致していれば、フォールトの発生個所が特定できない致命的な固定フォールトが発生したと判断し、その時点で運用を停止する手段と、を有することを特徴とする二重化情報処理装置である。

【0025】更にまた、ハードウェアを二重化した常用冗長コンピュータシステムにおいて、二重化された入出力構成要素(16, 26)を有し、それぞれの前記入出力構成要素(16, 26)どうしの出力の一一致を比較する手段(15, 25)と、該入出力構成要素(16, 26)の出力結果を記憶しておくための結果記憶装置(31, 41)と、前記比較結果に応じてシステムの運用構成を決定する手段と、を有することを特徴とする二重化情報処理装置である。

【0026】また、前記比較結果に応じてシステムの運用構成を決定する手段は、前記比較の結果、入出力構成要素(16, 26)の出力の不一致が検出された場合、入出力構成要素(16, 26)のどちらか一方でフォールトの発生が検出されていれば、フォールトの発生した入出力構成要素を切り離して縮退運用を行ない、フォールトの発生が検出されていなければ、それぞれの前記結果記憶装置(31, 41)に、入出力構成要素(16, 26)の出力を記憶した後、入出力処理の複数回の再実行を行ない、最初の再実行で、入出力構成要素(16, 26)の出力の一一致が確認されれば、フォールトは、過渡的なものと判断し、そのまま処理を継続し、再度、不

一致が検出された場合には、それぞれの入出力構成要素(16)の出力結果と結果記憶装置(31)に記憶しておいた結果とで、比較を行ない、入出力構成要素(16, 26)の一方が一致して、他方が一致していなければ、一致していない方の入出力構成要素を切り離して縮退運用を行ない、両方とも不一致であれば、原理的に二重化常用冗長コンピュータシステムでは対処できない二重の固定的または間欠的なフォールトが発生したと判断し、その時点で運用を停止し、両方とも一致していれば、指定された回数だけ再実行を繰り返し、全ての再実行において、入出力構成要素どうしに不一致があり、かつ結果記憶装置とも一致していれば、フォールトの発生個所が特定できない致命的な固定フォールトが発生したと判断し、その時点で運用を停止する手段と、を有することを特徴とする二重化情報処理装置である。

【0027】また、前記フォールトの発生箇所が特定できない場合に限り、前記再実行を行なう、ことを特徴とした二重化情報処理装置である。

【0028】【作用】本発明によれば、ハードウェアを二重化した常用冗長コンピュータシステムにおいて、情報処理構成要素または入出力構成要素のどちらか、もしくは両方に複数回の再実行と再実行前の結果との比較を可能とする構成を装備し、フォールトの発生個所が特定できない出力の不一致が生じた場合、複数回の再実行(時間冗長)を行なうことにより、フォールトの発生個所を特定可能とし、より高い信頼性のコンピュータシステムを実現することができる。

【0029】すなわち、本発明では、差分記憶装置12と差分記憶装置22、結果記憶装置13と結果記憶装置23により、情報処理構成要素11と情報処理構成要素21に不一致が発生した場合の再実行後の結果と、再実行前の結果との比較を可能としている。

【0030】また、結果記憶装置31と結果記憶装置41により、入出力構成要素16と入出力構成要素26に不一致が発生して再実行を行なった場合、再実行後の結果と再実行前の結果との比較を可能としている。

【0031】この再実行と再実行前の結果との比較を可能とすることにより、従来のハードウェアを二重化した常用冗長コンピュータシステムでは対処できなかった、フォールト発生個所の特定できない外乱要因による過渡フォールト、及びハードウェア故障と外乱要因の複合条件により発生する間欠フォールトの一部についても対応可能となり、より信頼性の高いコンピュータシステムを実現することができる。

【0032】また、フォールトの発生個所が特定できない場合に、複数回の再実行(時間冗長)を行なうことでの外乱要因による過渡フォールトについては、ほとんどの場合において、フォールトの発生個所を特定することが可能となり、縮退による継続運用が可能となる。

【0033】また、ハードウェア故障と外乱要因の複合

条件により発生する間欠フォールトについても、発生個所を特定できるケースがあり、信頼性の向上に大きく貢献する。

【0034】また、フォールトの発生個所が特定できない場合に限り、再実行(時間冗長)を行なう為、三重化以上のハードウェア冗長を行なう場合と比較して、明らかに製造コストを低く押さえることが可能となる。

【0035】また、再実行(時間冗長)による性能低下も、必要最小限に押さえることができる。

【0036】

【発明の実施の形態】図1は、本発明の構成を示す模式的構成図である。

【0037】図1において、同期・比較装置14と同期・比較装置24は、互いに協調し合い、情報処理構成要素11と情報処理構成要素21の動作を同期させると共に、情報処理構成要素11と情報処理構成要素21の動作が一致しているかの比較を行なう。

【0038】また、入出力構成要素16と入出力構成要素26の出力は、同期・比較装置14と同期・比較装置24を経由して、比較の結果が一致していれば、情報処理構成要素11と情報処理構成要素21に入力する。

【0039】さらに、情報処理構成要素11と情報処理構成要素21の出力は、比較装置15と比較装置25を経由して、比較の結果が一致していれば、入出力構成要素16と入出力構成要素26に入力する。

【0040】差分記憶装置12と差分記憶装置22は、それぞれ情報処理構成要素11と情報処理構成要素21の動作の一一致、または出力の一一致が確認された状態と、確認される前の状態との差分情報を記憶している。

【0041】もし、情報処理構成要素11と情報処理構成要素21の動作の一一致、または出力の一一致を検証した際に、不一致が検出された場合、情報処理構成要素11と情報処理構成要素21のどちらか一方でフォールトの発生が検出されていれば、フォールトの発生した情報処理要素を切り離して縮退運用を行なう。

【0042】フォールトの発生が検出されていなければ、結果記憶装置13と結果記憶装置23に情報処理構成要素11と情報処理構成要素21の状態を記憶した後、差分記憶装置12と差分記憶装置22の情報を元に、情報処理構成要素11と情報処理構成要素21を動作の一一致、または出力の一一致が確認される前の状態に戻し、複数回の再実行を行なう。

【0043】最初の再実行で、情報処理構成要素11と情報処理構成要素21の動作の一一致、または出力の一一致が確認されれば、フォールトは外乱要因による過渡的なものと判断し、そのまま処理を継続する。

【0044】しかし、再度、不一致が検出された場合は、それぞれ、情報処理構成要素11と結果記憶装置13、情報処理構成要素21と結果記憶装置23で比較を行ない、情報処理構成要素11と情報処理構成要素21

の一方が一致して、他方が一致していなければ、一致していない方の情報処理構成要素を切り離して縮退運用を行なう。

【0045】両方とも不一致であれば、二重の固定的または間欠的なフォールトが発生したと判断し、その時点で運用を停止する。

【0046】両方とも一致していれば、指定された回数だけ再実行を繰り返し、全ての再実行において、情報処理構成要素11と情報処理構成要素21に不一致があり、かつ結果記憶装置とも一致していれば、フォールトの発生個所が特定できない致命的な固定フォールトが発生したと判断し、その時点で運用を停止する。また、もし入出力構成要素16と入出力構成要素26の出力の一一致を検証した際に、不一致が検出された場合、入出力構成要素16と入出力構成要素のどちらか一方でフォールトの発生が検出されていれば、フォールトの発生した入出力構成要素を切り離して縮退運用を行なう。

【0047】フォールトの発生が検出されていなければ、結果記憶装置31と結果記憶装置41に、入出力構成要素16と入出力構成要素26の状態を記憶した後、入出力処理の複数回の再実行を行なう。

【0048】最初の再実行で、入出力構成要素16と入出力構成要素26の出力の一一致が確認されれば、フォールトは外乱要因による過渡的なものと判断し、そのまま処理を継続する。

【0049】しかし、再度、不一致が検出された場合には、それぞれ、入出力構成要素16と結果記憶装置31、入出力構成要素26と結果記憶装置41で比較を行ない、入出力構成要素16と入出力構成要素26の一方が一致して、他方が一致していなければ、一致していない方の入出力構成要素を切り離して縮退運用を行なう。

【0050】両方とも不一致であれば、二重の固定的または間欠的なフォールトが発生したと判断し、その時点で運用を停止する。

【0051】両方とも一致していれば、指定された回数だけ再実行を繰り返し、全ての再実行において、入出力構成要素16と入出力構成要素26に不一致があり、かつ結果記憶装置とも一致していれば、フォールトの発生個所が特定できない致命的な固定フォールトが発生したと判断し、その時点で運用を停止する。

【0052】このようにして、本願発明では、差分記憶装置12と差分記憶装置22、結果記憶装置13と結果記憶装置23により、情報処理構成要素11と情報処理構成要素21に不一致が発生した場合の再実行後の結果と、再実行前の結果との比較を可能としている。

【0053】また、結果記憶装置31と結果記憶装置41により、入出力構成要素16と入出力構成要素26に不一致が発生して再実行を行なった場合、再実行後の結果と再実行前の結果との比較を可能としている。

【0054】この再実行と再実行前の結果との比較を可

能とすることにより、従来のハードウェアを二重化した常用冗長コンピュータシステムでは対処できなかった、フォールト発生個所の特定できない外乱要因による過渡フォールト、及びハードウェア故障と外乱要因の複合条件により発生する間欠フォールトの一部についても対応可能となり、より信頼性の高いコンピュータシステムを実現することができる。

【0055】

【実施例】以下、本発明の実施例について説明する。

【0056】【構成の説明】図3を参照すると、本発明の一実施例としての二重化常用冗長コンピュータシステムが示されている。

【0057】図3において、同期・比較装置14と同期・比較装置24は、互いに協調し合い、複数のCPUとメモリにて構成される情報処理構成要素11と情報処理構成要素21の動作を、システムクロックまたは入出力割込みや、タイマー割込み、ソフトウェアのブレークポイントなどにより同期させると共に、情報処理構成要素11と情報処理構成要素21の動作が一致しているかの比較を行なう。

【0058】また、ディスクやネットワークなどで構成される入出力構成要素16と入出力構成要素26の出力は、同期・比較装置14と同期・比較装置24を経由して受け取られ、比較の結果が一致していれば、情報処理構成要素11と情報処理構成要素21に入力する。

【0059】さらに、情報処理構成要素11と情報処理構成要素21の出力は、比較装置15と比較装置25を経由して、比較の結果が一致していれば、入出力構成要素16と入出力構成要素26に入力する。

【0060】差分記憶装置12と差分記憶装置22は、それぞれ情報処理構成要素11と情報処理構成要素21の動作の一一致、または出力の一一致が確認された状態と、確認される前の状態との差分情報を記憶している。

【0061】もし、情報処理構成要素11と情報処理構成要素21の動作の一一致、または、出力の一一致を検証した際に、不一致が検出された場合、情報処理構成要素11と情報処理構成要素21のどちらか一方でフォールトの発生が検出されれば、フォールトの発生した情報処理構成要素を切り離して縮退運用を行なう。

【0062】フォールトの発生が検出されていなければ、結果記憶装置13と結果記憶装置23に情報処理構成要素11と情報処理構成要素21の状態を記憶した後、差分記憶装置12と差分記憶装置22の情報を元に、情報処理構成要素11と情報処理構成要素21を、動作の一一致、または出力の一一致が確認される前の状態に戻し、複数回の再実行を行なう。

【0063】最初の再実行で、情報処理構成要素11と情報処理構成要素21の動作の一一致、または出力の一一致が確認されれば、フォールトは、放射線や電磁ノイズなどの外乱要因による過渡的なものと判断し、そのまま処

理を継続する。

【0064】しかし、再度、不一致が検出された場合には、それぞれ、情報処理構成要素11の出力結果と結果記憶装置13に記憶されている結果、情報処理構成要素21の出力結果と結果記憶装置23に記憶されている結果とで比較を行ない、情報処理構成要素11と情報処理構成要素21の一方が一致して、他方が一致していなければ、一致していない方の情報処理構成要素を切り離して縮退運用を行なう。

【0065】両方とも不一致であれば、原理的に二重化常用冗長コンピュータシステムでは対処できない二重の固定的または間欠的なフォールトが発生したと判断し、その時点で運用を停止する。

【0066】両方とも一致していれば、指定された回数だけ再実行を繰り返し、全ての再実行において、情報処理構成要素11と情報処理構成要素21に不一致があり、かつ結果記憶装置とも一致していれば、フォールトの発生個所が特定できない致命的な固定フォールトが発生したと判断し、その時点で運用を停止する。切り離

された情報処理構成要素11または情報処理構成要素21は、診断および修理を行って正常であることを確認した後、システムに組み込まれる。この際には、正常動作している情報処理構成要素11または情報処理構成要素21の状態を、組み込まれた情報処理構成要素11または情報処理構成要素21にコピーした後、再度、同期・比較装置14と同期・比較装置24の動作を同期させ、冗長化された正常運用状態に移行する。

【0067】また、もし、入出力構成要素16と入出力構成要素26の出力の一一致を検証した際に、不一致が検

出された場合、入出力構成要素16と入出力構成要素26のどちらか一方でフォールトの発生が検出されれば、フォールトの発生した入出力構成要素を切り離して縮退運用を行なう。

【0068】フォールトの発生が検出されていなければ、結果記憶装置31と結果記憶装置41に入出力構成要素16と入出力構成要素26の状態を記憶した後、入出力処理の複数回の再実行を行なう。

【0069】最初の再実行で、入出力構成要素16と入出力構成要素26の出力の一一致が確認されれば、フォールトは、放射線や電磁ノイズなどの外乱要因による過渡的なものと判断し、そのまま処理を継続する。

【0070】しかし、再度、不一致が検出された場合には、それぞれ、入出力構成要素16と結果記憶装置31、入出力構成要素26と結果記憶装置41で比較を行ない、入出力構成要素16と入出力構成要素26の一方が一致して、他方が一致していなければ、一致していない方の入出力構成要素を切り離して縮退運用を行なう。

【0071】両方とも不一致であれば、原理的に二重化常用冗長コンピュータシステムでは対処できない二重の固定的または間欠的なフォールトが発生したと判断し、

その時点で運用を停止する。

【0072】両方とも一致していれば、指定された回数だけ再実行を繰り返し、全ての再実行において入出力構成要素16と入出力構成要素26に不一致があり、かつ、それぞれの結果記憶装置31, 41とも一致していれば、フォールトの発生個所が特定できない致命的な固定フォールトが発生したと判断し、その時点で運用を停止する。

【0073】切り離された入出力構成要素16と入出力構成要素26は、診断および修理を行って正常であることを確認した後、システムに組み込まれる。この際には、正常動作している入出力構成要素16と入出力構成要素26の状態や、ディスクのデータを、プライベートLANなどを介して組み込まれた情報処理構成要素11または情報処理構成要素21にコピーすることで、冗長化された正常運用状態に移行する。

【0074】【動作の説明】次に、図3の二重化常用冗長コンピュータシステムの動作を、図4、図5に示すフローチャートを使用して説明する。

【0075】図4において、通常実行を行なうと共に、差分記憶装置に前回の同期処理の時点からの差分情報を記憶する。

【0076】次に同期処理を行ない、情報処理構成要素11, 21の動作の一一致、または出力の一一致を検証する。

【0077】一致を確認した場合、引続き、通常実行を行なう。不一致を確認した場合、次に、情報処理構成要素11, 21のフォールト発生有無を検証し、一方の情報処理構成要素でフォールト発生を検出した場合、該当する情報処理構成要素を切り離して縮退運転に入る。

【0078】フォールトが発生していないことを確認した場合、結果記憶装置13, 23に不一致が発生している結果を記憶し、再実行回数カウンタ17, 27を0から1に変更する。

【0079】次に、差分記憶装置のデータを元に、情報処理構成要素11, 21を前回の同期処理の時点の状態に戻し、再実行回数カウンタが、規定数(この場合は2とする)を超えていないことを確認後、図5の①にある通り、再実行を行なう。

【0080】次に、同期処理を行ない、情報処理構成要素11, 21の動作の一一致、または出力の一一致を検証する。一致を確認した場合、再実行回数カウンタの値を0にして、図4の②にある通り、通常実行に戻る。

【0081】不一致を確認した場合、次に、情報処理構成要素11, 21のフォールト発生有無を検証し、一方の情報処理構成要素でフォールト発生を検出した場合、該当する情報処理構成要素を切り離して縮退運転に入る。

【0082】フォールトが発生していないことを確認した場合、情報処理構成要素11の出力結果と結果記憶装

置13に記憶していた結果、情報処理構成要素21の出力結果と結果記憶装置23に記憶していた結果について、動作の一一致、または出力の一一致を検証し、一方の情報処理構成要素で結果記憶装置との不一致を検出した場合、該当する情報処理構成要素を切り離して縮退運転に入る。一致を確認した場合、再実行回数カウンタ17, 27を1から2に変更する。

【0083】次に、差分記憶装置のデータを元に、情報処理構成要素11, 21を前回の同期処理の時点の状態10に戻し、再実行回数カウンタが、規定数(この場合は2とする)に達したことを確認後、運用を停止する。

【0084】入出力構成要素16, 26についても、基本動作は上記の情報処理構成要素11, 21と同様であるが、同期処理は行わず、一定時間待ち合わせた後に出力の一一致を検証する。

【0085】一致を確認した場合、引続き、通常実行を行なう。不一致を確認した場合、次に、入出力構成要素16, 26のフォールト発生有無を検証し、一方の入出力構成要素でフォールト発生を検出した場合、該当する入出力構成要素を切り離して縮退運転に入る。一定時間待ち合わせて出力が無い場合にもフォールト発生とみなす。

【0086】フォールトが発生していないことを確認した場合、結果記憶装置31, 41に不一致が発生している結果を記憶し、再実行回数カウンタ32, 42を0から1に変更する。

【0087】次に、再実行回数カウンタが、規定数(この場合は2とする)を超えていないことを確認後、入出力処理の再実行を行なう。

【0088】次に、一定時間待ち合わせた後に入出力構成要素16, 26の出力の一一致を検証する。一致を確認した場合、再実行回数カウンタの値を0にして、通常実行に戻る。

【0089】不一致を確認した場合、次に、入出力構成要素16, 26のフォールト発生有無を検証し、一方の入出力構成要素でフォールト発生を検出した場合、該当する入出力構成要素を切り離して縮退運転に入る。

【0090】フォールトが発生していないことを確認した場合、入出力構成要素16の出力結果と結果記憶装置40 31に記憶していた結果、入出力構成要素26の出力結果と結果記憶装置41に記憶していた結果について、出力の一一致を検証し、一方の入出力構成要素で結果記憶装置との不一致を検出した場合、該当する入出力構成要素を切り離して縮退運転に入る。一致を確認した場合、再実行回数カウンタ32, 42を1から2に変更する。

【0091】次に、入出力処理の再実行を行い、再実行回数カウンタが、規定数(この場合は2とする)に達したことを確認後、運用を停止する。

【0092】

【発明の効果】以上説明したように、本発明において

は、以下に記載するような効果を奏する。

【0093】第1の効果は、従来のハードウェアを二重化した常用冗長コンピュータシステムと比較して、フォールトの発生個所が特定できない場合に、複数回の再実行(時間冗長)を行なうことで、外乱要因による過渡フォールトについては、ほとんどの場合において、フォールトの発生個所を特定することが可能となり、縮退による継続運用が可能となる。

【0094】また、ハードウェア故障と外乱要因の複合条件により発生する間欠フォールトについても、発生個所を特定できるケースがあり、信頼性の向上に大きく貢献することである。

【0095】第2の効果は、ハードウェアを二重化した常用冗長コンピュータシステムにおいて、フォールトの発生個所が特定できない場合に限り、再実行(時間冗長)を行なう為、三重化以上のハードウェア冗長を行なう場合と比較して、明らかに製造コストを低く押さえることが可能となる。

【0096】また、再実行(時間冗長)による性能低下も、必要最小限に押さえることができる。

20

【図面の簡単な説明】

【図1】本発明の実施例の構成を示す模式的構成図である。

【図2】従来例の構成を示す模式的構成図である。

【図3】本発明の実施例の構成を示す模式的構成図である。

【図4】本発明の実施例の動作を示すフローチャートである。

【図5】本発明の実施例の動作を示すフローチャートである。

【符号の説明】

1 1, 2 1 情報処理構成要素

1 2, 2 2 差分記憶装置

1 3, 2 3 結果記憶装置

1 4, 2 4 同期・比較装置

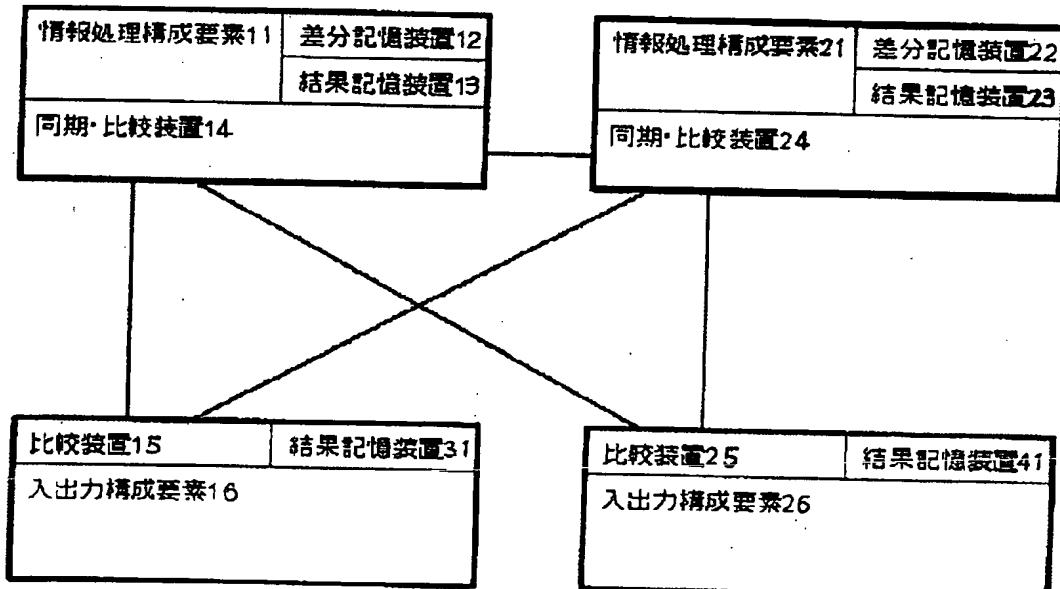
1 5, 2 5 比較装置

1 6, 2 6 入出力構成要素

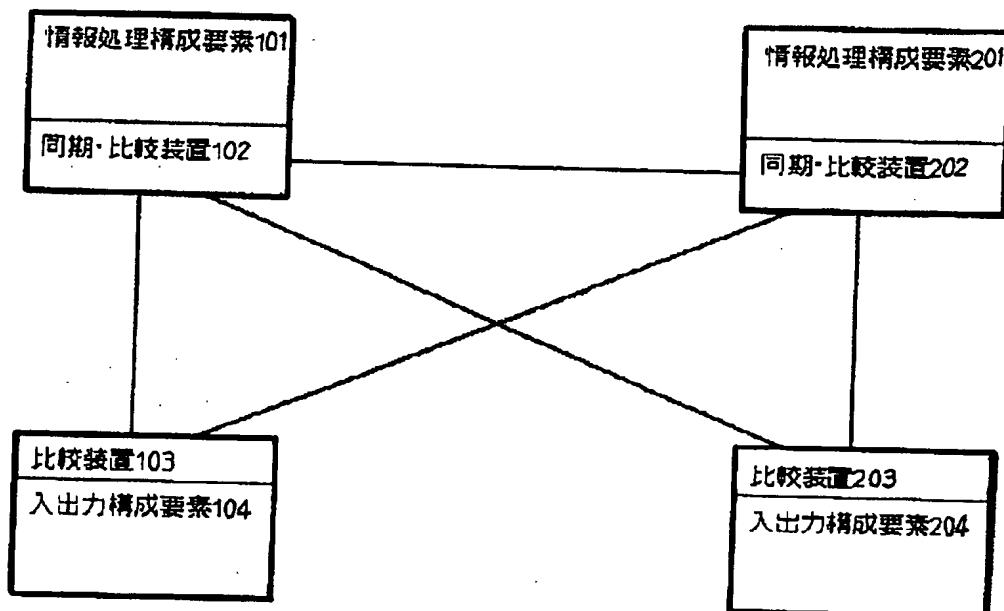
1 7, 2 7, 3 2, 4 2 再実行回数カウンタ

3 1, 4 1 結果記憶装置

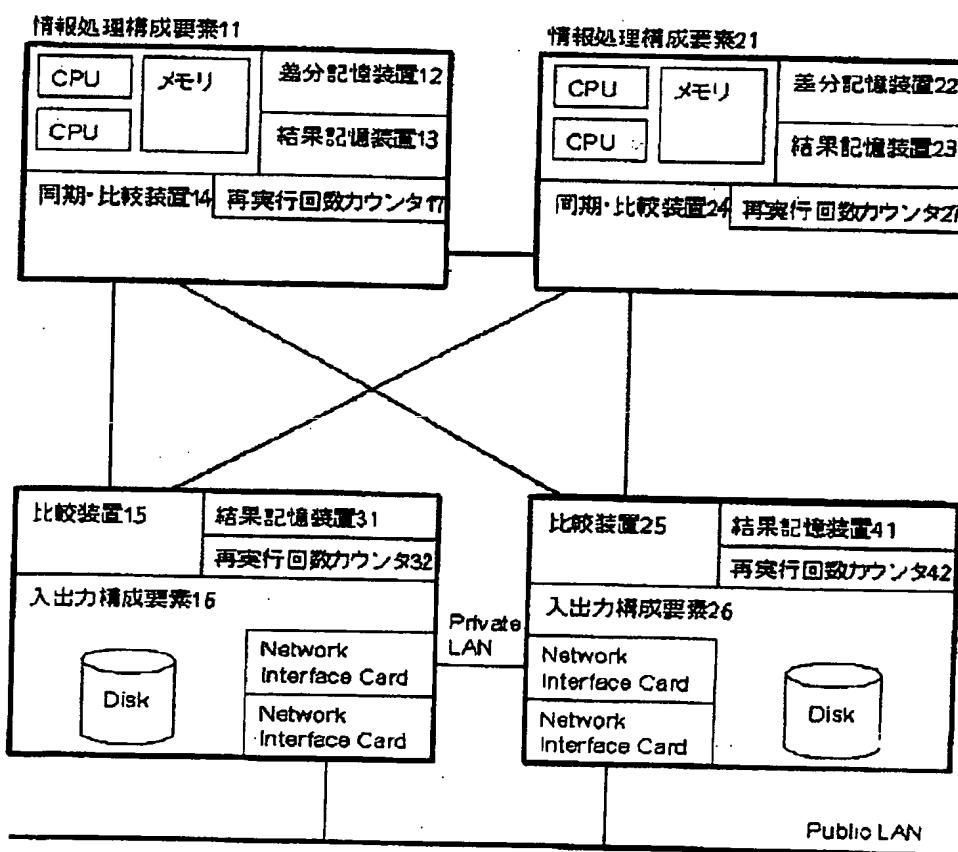
【図1】



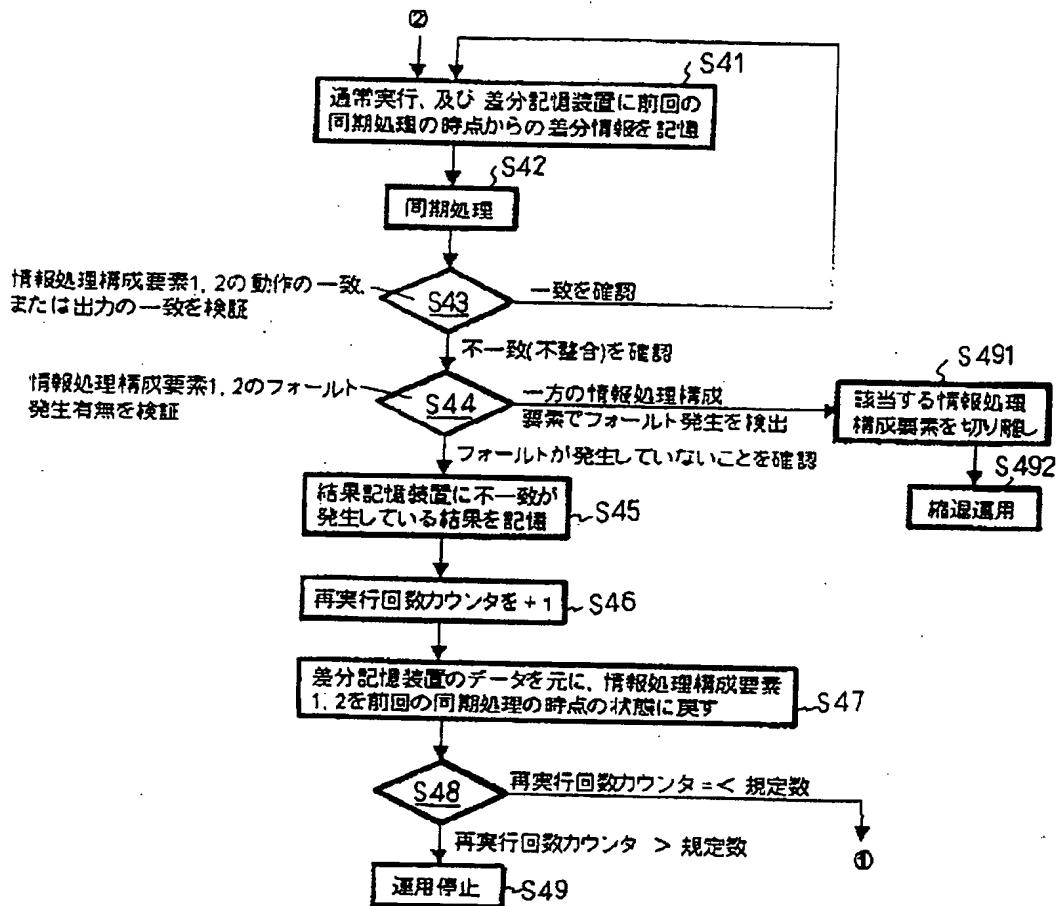
【図2】



【図3】



【図4】



【図5】

